WESTON COLLEGE

TRAINING SOLUTIONS

CYBER SECURITY TECHNICIAN

Introduction

The primary role of a Cyber Security Technician is to provide first line cyber security support. This requires individuals to monitor and detect potential security threats and escalate as necessary and to support secure and uninterrupted business operations of an organisation through the implementation of cyber security mechanisms and the application of cyber security procedures and controls.

Entry Requirements

There are no other formal qualifications required to start this apprenticeship but you will be assessed to ensure you have the ability to complete the English and Maths qualification to at least level 1.

You should hold a level 2 computing qualification to start this apprenticeship or have substantial workplace experience in a network security environment. You will also be assessed to ensure you have the ability to complete the English and maths qualifications at level 2.

Functional Skills

Apprentices will be required to have or achieve level 1 English and maths and taken the exams for level 2 prior to completion of their Apprenticeship. If Level 2 has already been achieved then development of further English and maths skills will continue for the whole of the apprenticeship.

Apprentices will be required to have or achieve level 2 English and maths prior to completion of their Apprenticeship. If this has already been achieved then development of further English and maths skills will continue for the whole of the apprenticeship.

Duration

18 months (this does not include EPA period).

Progression

This apprenticeship is recognised by the BCS - The Chartered Institute for IT at a Level of Associate BCS membership (AMBCS) and Professional. In addition, upon successful completion apprentices will also be able to apply for Registration for IT Technicians (RITTech). Additional there is recognition by the Chartered Institute for Information Security at an Accredited Affiliate.

Funding

Levy paying employers may fund apprentices on this programme from their Apprenticeship Account and non-levy paying SMEs through the co-funded option. There may be a small fee for some SME's.

End Point Assessment

To achieve this apprenticeship standard, the employer, training provider and apprentice will agree when the apprentice is ready and competent to undertake the i ndependent end assessment, which will test their skills knowledge and behaviours required for this role.

The EPA must be completed within an EPA period lasting typically 3 months, after the EPA gateway. The EPA consists of 3 discrete assessment methods.

MILESTONES

Pre sign up

Review workplace duties and relevance of data analyst role

- Initial assessment test
- Induction and sign-up paperwork completed
- Discuss taught sessions and identify schedule and 20% off the job training

Introduce My I.D.

Identify suitable workplace mentor

Employer Agreement

English and maths assessment

Smart Assessor orientation for employer and apprentice

Month 1

Basic security concepts and theory

Application of Information Security Policies and Procedures

Complete first unit of My I.D. – Apprenticeship Hub

Employer and apprentice discussion on 20% off the job training hours and time log.

Complete first Functional skill if required

Introduce Behaviours tracker

Health and Safety

Maths and English initial assessment

Month 2

Basic security concepts and theory (cont.)

Cyber security awareness and culture

Internal and external stakeholders

Complete second unit of My I.D.

Complete first Functional skill if required

Update behaviours tracker

Month 3

Maintaining professional knowledge of cyber security developments

Awareness of how current legislation relates to or impacts upon the occupation and the ethical use of information assets

Complete third unit of My I.D.

Complete first Functional skill if required

Employer and apprentice discussion on 20% off the job training hours and time log.

Update behaviours tracker

Month 4

Core terminology of cyber security

Confidentiality, integrity, availability (the CIA triad), assurance, authenticity, identification, authentication, authorization, accountability, reliability, nonrepudiation, access control

Complete fourth unit of My I.D.

Update behaviours tracker

Complete first Functional skill if required

Month 5

Information security governance practice.

Identify the business impact including mitigation for management risk

Complete fifth unit of My I.D.

Employer and apprentice discussion on 20% off the job training hours and time log.

Update behaviours tracker

Complete second Functional skill if required

Month 6

Cyber security operational tasks

Identify the categories of cyber security vulnerabilities and common vulnerability exposures

Complete sixth unit of My I.D.

Update behaviours tracker

Complete second Functional skill if required

Month 7

Modify a cyber security access control

Types of information security events – brute force attack, malware activity, suspicious user behaviour, suspicious device behaviour, unauthorized system changes

Employer and apprentice discussion on 20% off the job training hours and time log.

Update behaviours tracker

Complete second Functional skill if required

Month 8

Scope a cyber security vulnerability assessment

Responds and reports whilst preserving the chain of evidence

Update behaviours tracker

Complete second Functional skill if required

Month 9

Cyber security vulnerability assessment

How to evaluate the results of an assessment

Conducting a risk assessment

Employer and apprentice discussion on 20% off the job training hours and time log.

Update behaviours tracker

Month 10

Identify and categorises sources of threats and risk

Update behaviours tracker

Month 11

Security awareness within organisations and society

Employer and apprentice discussion on 20% off the job training hours and time log.

Update behaviours tracker

Month 12

Information security risk assessment

Main components of the organisation's information security

Update behaviours tracker

Month 13

An effective service desk

Identify and understanding of limits of their authority for action.

Employer and apprentice discussion on 20% off the job training hours and time log.

Update behaviours tracker

Preparation for EPA synoptic and professional discussion

Month 14

Ethical use of data

Update behaviours tracker

Preparation for EPA synoptic and professional discussion

Month 15

Mitigation(s) for the management of risk and business impact

Cyber security policies and procedures

Employer and apprentice discussion on 20% off the job training hours and time log.

Update behaviours tracker

Preparation for EPA synoptic and professional discussion

Month 16

Corporate cyber security culture

Update behaviours tracker

Preparation for EPA synoptic and professional discussion

Month 17

Maintaining a digital information asset inventory

Conducting and maintaining of a digital information asset inventory. The process to securely dispose of an information asset

Employer and apprentice discussion on 20% off the job training hours and time log.

Update behaviours tracker

Preparation for EPA synoptic and professional discussion

Month 18

Gateway’ to final assessment: Line Manager and Training Provider review progress and agree whether apprentice has achieved competency levels required against all learning outcomes.

Update behaviours tracker

Preparation for EPA synoptic and professional discussion

Month 19-21

Assessment method 1: Scenario Demonstrations with questioning

Assessment method 2: Professional Discussion underpinned by Portfolio

Assessment method 3: Knowledge Test

Occupation Duties	
Duty 1	Apply procedures and controls to maintain security and control of an organisation.
Duty 2	Contribute to the production and development of security culture across an organisation including assisting with the promotion of cyber security awareness programmes, monitoring the effectiveness of cyber security awareness programmes, promoting an effective cyber security culture
Duty 3	Process cyber security helpdesk requests ensuring confidentiality, integrity and availability of digital information, meeting relevant legal and regulatory requirements for example access control requests
Duty 4	Conduct the installation and maintenance of technical security controls in accordance with relevant procedures and standards
Duty 5	Monitor, identify, report and escalate information security incidents and events in accordance with relevant procedures and standards
Duty 6	Administer cryptographic and certificate management activities in accordance with relevant procedures and standards
Duty 7	Conduct regular review of access rights to digital information assets in accordance with relevant procedures and standards
Duty 8	Maintain an asset register of controlled environments in accordance with relevant policies, procedures and standards
Duty 9	Assist with backup and recovery processes in accordance with relevant policies, procedures and standards
Duty 10	Contribute to documenting the scope and evaluating the results of vulnerability assessments in accordance with management requirements
Duty 11	Contribute to risk assessments and escalate where appropriate in accordance with relevant procedures and standards
Duty 12	Contribute to routine threat intelligence gathering tasks
Duty 13	Document incident and event information and incident, exception and management reports in accordance with relevant policies, procedures and standards
Duty 14	Contribute towards the production and review of cyber security policies, procedures, standards and guidelines drawing on their experience of applying policies for example - acceptable use, incident management, patching, anti-virus, bring your own device (BYOD), access control, social media, password, data handling and data classification, information technology asset disposal

Duty 15	Monitor cyber security compliance and provide relevant data to auditors if required by the auditor
Duty 16	Collaborate with people both internally and externally to support secure and uninterrupted business operations of an organisation
Duty 17	Practice continuous self-learning to keep up to date with industry trends and developments to enhance relevant skills and take responsibility for own professional development
Duty 18	Monitor and detect potential security threats and escalate in accordance with relevant procedures and standards

END POINT ASSESSMENT

Readiness for the independent end assessment:

An apprentice will be put forward for end point assessment when they are in the best possible position to achieve success. The apprentice must meet all the duties as well as complete their 20% off the job training.

Functional Skills:

Level 2 English and maths must be achieved to progress on to the End Point Assessment.

Assignments:

Apprentices will have their knowledge and technical understanding formally assessed at relevant times during their apprenticeship through reviews with an assessor. Apprentices will have produced a portfolio of work-based assignments and projects to submit as part of the End Point Assessment. This will be supported by a summative portfolio template to outline the evidence for the end point assessor.

Subject specific assessments

The EPA will consist of three methods of assessment:

- Scenario Demonstrations with questioning: Apprentices must be observed by an independent assessor completing 4 practical tasks that would naturally occur as a Cyber Security Technician. Each scenario will last 75 minutes, and the independent assessor can ask up to 5 questions during and after each scenario demonstration during the 75 minutes permitted
- Professional Discussion underpinned by Portfolio: The professional discussion must last for 60 minutes. The independent assessor will ask a minimum of 10 questions and is a structured one-to-one discussion between the apprentice and the independent assessor
- Knowledge Test: Apprentices must have a maximum of 60 minutes to complete the test which consists of 40 closed response questions